(5) NE-1045

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－92046
（P2000－92046A）
(43)公開日　平成12年３月31日(2000.3.31)

| (51)Int.Cl.' | | 識別記号 | FI | | テーマコード'(参考) |
|---|---|---|---|---|---|
| H04L | 9/32 | | H04L | 9/00 | 673D 5B043 |
| G06F | 15/00 | 330 | G06F | 15/00 | 330F 5B085 |
| G06T | 7/00 | | | 15/62 | 460 5J104 |
| H04L | 9/14 | | H04L | 9/00 | 641 |
| | | | | | 673A |

審査請求　未請求　請求項の数７　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－257813

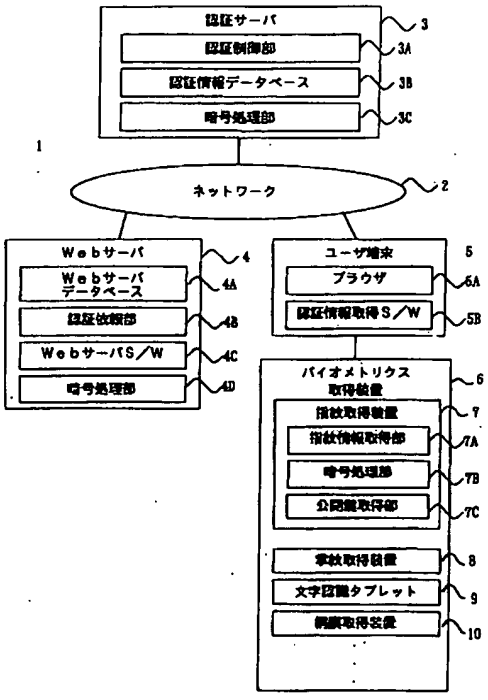
(22)出願日　平成10年９月11日(1998.9.11)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　中村　浩
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　馬場　義昌
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外２名）

最終頁に続く

(54)【発明の名称】　遠隔認証システム

(57)【要約】
【課題】　バイオメトリクス情報により個人の認証を行う際、ユーザの個人情報であるバイオメトリクス情報を保護した上で確実に認証が受けられるとともに、セキュリティ上強固な遠隔認証システムおよび遠隔認証方法を得る。
【解決手段】　ユーザの個人情報であるバイオメトリクス情報を暗号化し、バイオメトリクス情報はユーザの指定した認証サーバにのみ復号可能な状態でネットワーク上を転送するので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できると共に、認証サーバで認証情報作成時の日時が確認できるため、不正な認証情報の再使用が防止でき、さらに認証サーバによって認証されたかが認証依頼側で確認できるためシステムのセキュリティを高く保つことが可能である。



1

【特許請求の範囲】

【請求項１】　ネットワークに、認証サーバと、アプリケーションサーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、

前記認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、

前記ユーザ端末には少なくとも１つ又は複数種類のバイオメトリクス取得装置が接続され、

前記バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、

日時情報を取得し、日時情報と前記共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに前記共通鍵で暗号化し、

ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、

暗号化した前記バイオメトリクス情報と暗号化した前記共通鍵と日時情報と、日時情報と前記共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送し、

前記ユーザ端末と前記アプリケーションサーバは、該認証情報を前記認証サーバへ転送し、前記認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを前記秘密鍵で暗号化し、共に前記アプリケーションサーバに転送することを特徴とする遠隔認証システム。

【請求項２】　ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、前記認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも１つ又は複数種類のバイオメトリクス取得装置が接続され、

前記バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する前記認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、前記暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送し、

前記ユーザ端末は該認証情報を前記認証サーバへ転送し、

前記認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを前記秘密鍵で暗号化し、共に前記ユーザ端末に転送することを特徴とする遠隔認証システム。

2

【請求項３】　前記バイオメトリクス取得装置は、認証に際して、暗号化せずにバイオメトリクス情報を前記ユーザ端末へ転送し、

前記ユーザ端末は、取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに前記共通鍵で暗号化すると共に、前記暗号化したバイオメトリクス情報と前記暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として前記ユーザ端末へ転送することを特徴とする請求項１または請求項２に記載の遠隔認証システム。

【請求項４】　前記ユーザ端末は、認証に際して、取得したユーザのバイオメトリクス情報を暗号化する共通鍵暗号方式の共通鍵を生成する場合、前記共通鍵生成ための乱数の一部または全部に該バイオメトリクス情報を使用することを特徴とする請求項１～３のいずれかに記載の遠隔認証システム。

【請求項５】　前記バイオメトリクス取得装置は、バイオメトリクス取得装置を管理する管理者の認証部と、バイオメトリクス取得装置を初期化する初期化者の認証部を含み、

前記２つの認証部は独立して認証し、前記管理者が認証されない場合でも、前記初期化者の認証で初期化することを特徴とする請求項１～３のいずれかに記載の遠隔認証システム。

【請求項６】　前記認証サーバは、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定しない場合には、前回までのユーザを本人と同定した時の平均照合率と比較し、今回の照合率が前記管理者の定める規定値以上に大きく変動しているかを確認し、該既定値以上の大きな変動での失敗回数が前記管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知することを特徴とする請求項１～３のいずれかに記載の遠隔認証システム。

【請求項７】　前記認証サーバは、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定した場合には、前回までのユーザを本人と同定した時の照合率と比較し、同一の照合率であり、バイオメトリクス情報のメッセー

ジダイジェストが格納されていない場合にはユーザ認証を失敗させ、今回のバイオメトリクス情報のメッセージダイジェスト算出し、照合率とともに記憶し、同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出して照合率と組で記憶するとともに、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同定し、今回の照合率とメッセージダイジェストの組が過去の照合率とメッセージダイジェストの組と完全に一致した場合には本人と同定しないとともに、過去の照合率とメッセージダイジェストの組と完全に一致する場合が、管理者が定める既定値以上に達した場合には、予め登録されている連絡先に通知することを特徴とする請求項１～３のいずれかに記載の遠隔認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、バイオメトリクスにより個人の特定を行う遠隔認証システムに関するものである。

【０００２】

【従来の技術】従来、ネットワークに接続された情報処理システムにおいて機密保持のため、個人を特定し該個人のアクセス許可と不許可の判断を行なう、すなわち認証が必要である。また、銀行の現金自動支払い機等では個人の特定と預金残高など該個人の取り引き情報にアクセスするための認証や、機密度の高い研究場所や会員制クラブなどへの入退室時にも個人の認証が実施されている。

【０００３】これらの認証として、身分証明書などと同様の位置づけである、磁気カードやＩＣカードやパスワードなどの個人の記憶やこれらの組み合わせによって個人の特定と資格の認定、すなわち認証を実施している。パスワードなどは忘却の恐れや、磁気カード、ＩＣカードなどは紛失、破壊などにより認証が不能に陥ったり、盗難やパスワード情報の漏洩により本人以外が本人と成りすまして認証されてしまうなどの問題がある。

【０００４】また、ネットワーク上でユーザを認証する手段の１つに、ユーザの作成したメッセージを認証し、間接的にユーザを認証するデジタル署名がある。デジタル署名では、まずメッセージの送り手がメッセージの原文を圧縮したメッセージダイジェストを送り手の暗号鍵で暗号化した暗号文をメッセージに添付する。メッセージの受け手は、受け取ったメッセージからメッセージダイジェストを作成し、また送り手の復号鍵で添付された暗号文からメッセージダイジェストを復号してこれら２つのメッセージダイジェストが一致することで、送り手本人が送ったメッセージであることと、改竄されていないことを確認する。

【０００５】また、前記暗号方式には、暗号鍵と復号鍵



に同一の鍵を用いる共通鍵暗号方式と暗号鍵と復号鍵とが異なる公開鍵暗号方式が存在する。公開鍵暗号方式では、一方の鍵を秘密鍵とし安全に保管し、もう一方の鍵を公開鍵として公表する場合、公開鍵で暗号化された暗号文は秘密鍵を所持していなければもとのメッセージへ復号できないため、送り手は希望する受け手にのみ復号できる形でメッセージを転送でき、秘密鍵で暗号化された暗号文は公開鍵でもとのメッセージへ復号ができるため、秘密鍵を所持している送り手本人からのメッセージであることを受け手が認証できる。

【０００６】

【発明が解決しようとする課題】従来、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）のＲＦＣ（Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔ）に登録されているＲＦＣ１４２１，ＲＦＣ１４２２（ＰＥＭ：Ｐｒｉｖａｃｙ Ｅｎｈａｎｃｅｍｅｎｔ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｅｌｅｃｔｒｏｎｉｃ Ｍａｉｌ）では、前記デジタル署名とメッセージの暗号化を公開鍵暗号方式と共通鍵暗号方式によって行っているが、送り手は自分の秘密鍵を使用するため、送り手の責任で秘密鍵を管理する必要あり、例えばフロッピーディスクや磁気カード、ＩＣカードなどに格納して安全に所持しなければならないという問題があった。

【０００７】一方、指紋情報、掌紋情報、筆跡情報、網膜情報など個人の生体的特徴であるバイオメトリクス情報による認証では、成りすましが困難であることと、ユーザ本人がいれば前記秘密鍵の情報などを管理する必要がなく、また前記磁気カードやＩＣカードなどで個人を認証する場合の携行品所持の煩雑さや紛失による脅威や、前記パスワード認証時の記憶の煩雑さを解消できるが、バイオメトリクス情報による認証が広域で必要な場合には、集中的なバイオメトリクス情報の管理と認証する機器が必要であり、プライバシー保護の面からユーザのバイオメトリクス情報を認証を行う機器に転送する際には秘匿などを行いセキュリティを確保しなければならないという問題があった。

【０００８】また、バイオメトリクス情報を秘匿するために使用する暗号鍵を生成するようなシステムでは、一般に暗号鍵の生成に乱数を使用するが、該暗号鍵の解読を困難にするためには該乱数の傾向をなくすことが重要であるという問題もある。

【０００９】また、バイオメトリクスを取得する装置は、ユーザのプライバシーの保護の面から適切に管理しなければならなく、管理者の認証を行う必要があるが、この管理者の認証にバイオメトリクスを用いた場合には管理者の代行が他人はできないため、他の人は初期化も含め、バイオメトリクス取得装置に全くアクセスできなくなるという問題があった。また、正当な管理者であっても認証に使用しているバイオメトリクスが事故により傷害を受け、大きく変わってしまったり、なくなってしま

5

う場合などには正当な管理者であっても、初期化を含め、バイオメトリクス取得装置に全くアクセスできなくなるという問題があった。

【００１０】また、一般にユーザ認証を行うシステムでは、不正な認証を早期発見が求められ、例えば銀行のキャッシュカードなどでは規定回数パスワードによる認証が失敗すると該キャッシュカードを使用不能にするなどの手段を持っている。バイオメトリクスによりユーザを認証するシステムでも、不正な認証を早期発見する必要があるが、個人毎にバイオメトリクスの状態が異なり、例えば指紋照合により個人を認証するシステムでは、本人と同定する最低の照合率が決まっているが、指が荒れていたり磨り減っている人などはその時点で最良のバイオメトリクス情報が取得できても照合率低く、指の密着不足などちょっとした取得時の失敗によりさらに照合率が低下すると、認証自体が失敗する確立が高くなり、全ての人に対して規定回数だけで不正認証と判断することが公平にできないという問題があった。

【００１１】この発明は前記のような問題点を解決するためになされたもので、バイオメトリクス情報により個人の認証を行う際、ユーザの個人情報であるバイオメトリクス情報を保護した上で確実に認証が受けられるとともに、セキュリティ上強固な遠隔認証システムおよび遠隔認証方法を得ることを目的とする。

【００１２】

【課題を解決するための手段】第１の発明に係る遠隔認証システムは、ネットワークに認証サーバと、アプリケーションサーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、認証サーバは公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも１つ又は複数種類のバイオメトリクス取得装置が接続され、バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報としてユーザ端末へ転送し、ユーザ端末とアプリケーションサーバは、該認証情報を認証サーバへ転送し、認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを秘密鍵で暗号化し、共にアプリケーションサーバに転送するものである。

6

【００１３】また、第２の発明に係る遠隔認証システムは、ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、前記ユーザ端末を使用するユーザの認証を行う遠隔認証システムにおいて、認証サーバは、公開鍵暗号方式の公開鍵と秘密鍵の組を所持し、公開鍵を公開し、秘密鍵を秘匿しており、前記ユーザ端末には少なくとも１つ又は複数種類のバイオメトリクス取得装置が接続され、バイオメトリクス取得装置は、認証に際して取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報としてユーザ端末へ転送し、ユーザ端末は該認証情報を認証サーバへ転送し、認証サーバは、転送された認証情報を前記秘密鍵で復号を行って得た前記共通鍵により、ユーザのバイオメトリクス情報を復号し、該バイオメトリクス情報によってユーザを認証し、認証した結果と認証した結果のメッセージダイジェストを秘密鍵で暗号化し、共にユーザ端末に転送するものである。

【００１４】また、第３の発明に係る遠隔認証システムは、バイオメトリクス取得装置が、認証に際しては、暗号化せずにバイオメトリクス情報をユーザ端末へ転送し、ユーザ端末が取得したユーザのバイオメトリクス情報を、共通鍵暗号方式の共通鍵で暗号化し、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化し、ユーザの指定する認証サーバの公開鍵を取得し、前記共通鍵を前記認証サーバの公開鍵で暗号化すると共に、暗号化したバイオメトリクス情報と暗号化した共通鍵と日時情報と、日時情報と共通鍵を連結してメッセージダイジェストを暗号化したものを認証情報として転送するものである。

【００１５】また、第４の発明に係わる遠隔認証システムは、認証に際して、取得したユーザのバイオメトリクス情報を暗号化する共通鍵暗号方式の共通鍵を生成するための乱数の一部または全部に該バイオメトリクス情報を使用するものである。

【００１６】第５の発明に係わる遠隔認証システムは、バイオメトリクス取得装置が、バイオメトリクス取得装置を管理する管理者の認証部と、バイオメトリクス取得装置を初期化する初期化者の認証部を含み、前記２つの認証部は独立して認証し、管理者が認証されない場合でも、初期化者の認証で初期化だけは実施できるものである。

【００１７】第６の発明に係わる遠隔認証システムは、

認証サーバが、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定しない場合には、前回までのユーザを本人と同定した時の平均照合率と比較し、今回の照合率が管理者の定める規定値以上に大きく変動しているかを確認し、該既定値以上の大きな変動での失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知するものである。

【００１８】また、第７の発明に係わる遠隔認証システムは、認証サーバが、ユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴を記憶し、ユーザ認証に際して、本人と同定した場合には、前回までのユーザを本人と同定した時の照合率と比較し、同一の照合率であり、バイオメトリクス情報のメッセージダイジェストが格納されていない場合にはユーザ認証を失敗させ、今回のバイオメトリクス情報のメッセージダイジェスト算出し、照合率とともに記憶し、同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出して照合率と組で記憶するとともに、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同定し、今回の照合率とメッセージダイジェストの組が過去の照合率とメッセージダイジェストの組と完全に一致した場合には本人と同定しないとともに、過去の照合率とメッセージダイジェストの組と完全に一致する場合が、管理者の定める既定値以上に達した場合には、予め登録されている連絡先に通知するものである。

【００１９】

【発明の実施の形態】以下図面を参照してこの発明の実施の形態を詳述する。

【００２０】実施の形態１．図１にこの発明を適用したＷｅｂシステム１の構成を示す。ネットワーク２上に認証サーバ３、個人認証を必要とするアプリケーションサーバであるＷｅｂサーバ４、ユーザ端末５が接続され、ユーザ端末５にバイオメトリクス取得装置６が接続される。このＷｅｂシステム１において、ユーザがユーザ端末５を通じてＷｅｂサーバ４にアクセスした場合に、Ｗｅｂサーバ４はそのユーザの個人認証を認証サーバ３から受け、その結果によりユーザに対してアクセス制御を行う。

【００２１】認証サーバ３は、認証制御部３Ａ、暗号処理部３Ｃと、認証情報データベース３Ｂから構成されるパーソナルコンピュータやワークステーション等のコンピュータ装置（以下構成としてＣＰＵ、メモリ、ディスク、通信制御等を有するものを示す）であり、公開鍵方式の一方の鍵を公開鍵として公開し、もう一方を秘密鍵として秘匿している。

【００２２】また、Ｗｅｂサーバ４は、Ｗｅｂサーバデータベース４Ａ、暗号処理部４Ｄ、認証依頼部４Ｂと、個人認証を必要とするアプリケーションであるＷｅｂサーバソフトウェア４Ｃ（以下ソフトウェアは、Ｓ／Ｗと記述する）のアプリケーションが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【００２３】また、ユーザ端末５は、Ｗｅｂサーバ端末４の情報を表示するブラウザ５Ａと、認証情報取得Ｓ／Ｗ５Ｂが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末５には、バイオメトリクス取得装置６が接続されている。バイオメトリクス取得装置６は、画像処理等により人体の指紋や掌紋情報をバイオメトリクス情報として取得する、指紋取得装置７や、掌紋取得装置８、ユーザが描いた筆跡情報をバイオメトリクス情報として取得する文字認識タブレット９、眼底スキャンに等によって人体の網膜情報をバイオメトリクス情報として取得する網膜取得装置１０等を示している。

【００２４】ここでは、バイオメトリクス取得装置６に指紋取得装置７を使用する場合を例として説明する。また、指紋取得装置７などバイオメトリクス取得装置６の取得するバイオメトリクス情報は、画像データや、静電データなど加工されていないイメージデータであっても、イメージデータから特徴などを抽出した特徴点データであってもよい。指紋取得装置７は、画像処理等により、指紋情報を取得し、ユーザ端末に転送する指紋情報取得部７Ａと、指紋情報を暗号化する暗号処理部７Ｂと、認証サーバ３の公開鍵を取得する公開鍵取得部７Ｃから構成される。

【００２５】次に動作について説明する。このようなＷｅｂシステム１における認証処理の流れを図２に示す。まずユーザがユーザ端末５で動作しているアプリケーションであるブラウザ５Ａにより、Ｗｅｂサーバ４の機密度の高いＷｅｂサーバデータベース４Ａの情報にアクセスした場合（ＳＰ５）について説明する。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証をする必要がある。

【００２６】ユーザ端末５の認証情報取得Ｓ／Ｗ４Ｃは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋取得装置７から取得する（ＳＰ６）。この時他のＳ／Ｗ（認証情報を取得するドライバなどのソフトウエア）と協調して動作する場合もある。

【００２７】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂから指紋情報の取得を指示された、指紋取得装置７の指紋情報取得部７Ａは、ユーザから指紋情報を取得する（ＳＰ１）。この指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部７Ｂで暗号化を実施するが、まず暗号処理部７Ｂは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報

を暗号化する。同時に暗号処理部７Ｂは、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する（ＳＰ２）。指紋取得装置７の公開鍵取得部７Ｃは、フロッピーディスクや、磁気カード、ＩＣカード、またはキー入力などユーザからの指示により認証サーバの公開鍵を得る。または指紋取得装置７が適切に管理されている場合には、認証サーバ３の公開鍵が指紋取得装置７で固定的に公開鍵取得部７Ｃに格納されており、ユーザが認知した上でその公開鍵を用いる場合もある。次に暗号処理部７Ｂは前記共通鍵を認証サーバ３の公開鍵で暗号化する（ＳＰ３）。そして、指紋取得部７Ａは、暗号化された指紋情報と、日時情報と、暗号化された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報としてユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂに転送する（ＳＰ４）。

【００２８】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂは、ブラウザ５Ａを介してＷｅｂサーバ４へ取得した認証情報を転送する。この時、ブラウザ５Ａは別途取得したユーザ名やメールアドレスなどのユーザＩＤを認証情報に追加して転送する（ＳＰ７）。

【００２９】Ｗｅｂサーバ４の認証依頼部４Ｂは、ＷｅｂサーバＳ／Ｗ４Ｃを介して取得した認証情報を認証サーバ３の認証制御部３Ａへ転送する（ＳＰ９）。

【００３０】認証サーバ３の認証制御部３Ａは転送された認証情報を暗号処理部３Ｃで復号させ、ユーザ認証を実施する。この時暗号処理部３Ｃでは、認証サーバ３で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する（ＳＰ１２）。認証制御部３Ａは転送された認証情報に含まれる指紋情報とユーザIDと、認証サーバ３の認証情報データベース３Ｂに元々蓄積されている個人情報から指紋照合を実施する。認証制御部３Ａは、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部３Ｃに引き渡され、暗号処理部３Ｃでは認証結果のメッセージダイジェストをとり、認証サーバ３の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部３Ａへ引き渡す。認証制御部３Ａは前記暗号化されたメッセージダイジェストを認証結果に含めてＷｅｂサーバ４の認証依頼部４Ｂへ通知する（ＳＰ１３）。

【００３１】認証結果を受けたＷｅｂサーバ４の認証依頼部４Ｂは、暗号処理部４Ｄに認証結果を通知する。暗号処理部４Ｄは通知された暗号化されたメッセージダイジェストを認証サーバ３の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することにより、確かに正当な認証サーバ３からの通知であることを確認する（ＳＰ１０）。認証依頼部４Ｂは正当な認証サーバ３からの通知であることを確認したことを暗号処理部４Ｄから知らされたならば認証結果をＷｅｂサーバＳ／Ｗ４Ｃに通知する。ＷｅｂサーバＳ／Ｗ４Ｃは該認証結果により該ユーザに対してＷｅｂサーバデータベース４Ａの機密度の高い情報へのアクセス許可・不許可を判定する（ＳＰ１１）。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう。

【００３２】このように、ユーザの個人情報である指紋情報は生成した共通鍵で暗号化され、該共通鍵は、ユーザが設定した認証サーバ３の公開鍵により暗号化されることと、認証サーバ３の公開鍵は指紋取得装置７にユーザが直接設定するため、指紋情報はユーザの指定した認証サーバ３にのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報である指紋情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果がある。さらに、ユーザは認証サーバ３の公開鍵のみをフロッピーディスクや、磁気カード、ＩＣカード、またはキー入力などで指紋取得装置７に指示できるようにすればよく、この公開鍵を格納しているフロッピーディスクや、磁気カード、ＩＣカードなどが紛失や盗難にあってもセキュリティ上問題がなく、同じ公開鍵を格納した代替え品や同一品により個人認証を受けることができる。この公開鍵を格納している代替え品はユーザ毎に管理されているものではないため、紛失や盗難時に特別な届け出や再発行などの処理が不要であり、管理負荷が軽減できるという効果もある。

【００３３】また、認証サーバ３で認証情報作成時の日時が確認するため、不正な認証情報の再使用が防止でき、認証情報認証サーバ３によって認証されたかが認証依頼側のＷｅｂサーバ４で確認できるためセキュリティを高く保つことが可能である。

【００３４】本実施例ではＷｅｂシステム１に適用した例を示したが、ＷｅｂサーバＳ／Ｗ４Ｃとブラウザ５Ａが、例えば経理情報管理サーバＳ／Ｗと経理情報管理クライアントＳ／Ｗであったり、データベース検索サーバＳ／Ｗとデータベース検索クライアントＳ／Ｗなど他のシステムを構成するアプリケーションであっても同様な効果が得られる。

【００３５】実施の形態２．この実施の形態２においては実施の形態１を簡略したものであり、図１のＷｅｂサーバ４とユーザ端末５は図３のユーザ端末５の１つになる。図１との対応部分に同一符号を付けた図３では、個人認証を必要とするアプリケーションがユーザ端末５にのみ存在するため、図１のＷｅｂサーバＳ／Ｗ４Ｃとブラウザ５Ａのシステムを構成する２つのアプリケーションが１つのデータベース検索Ｓ／Ｗ５Ｅに置き換わり、ＷｅｂサーバデータベースＡはローカルデータベース

５Ｃに置き換わる場合である。この場合図１のＷｅｂサーバ４を構成していた認証依頼部４Ｂと暗号処理部４Ｄは、図３のユーザ端末５の構成部位となる。

【００３６】実施の形態２においては、ユーザ端末５は、ローカルデータベース５Ｃ、暗号処理部５Ｆ、認証依頼部５Ｄと、個人認証を必要とするアプリケーションであるデータベース検索Ｓ／Ｗ５Ｅ、認証情報取得Ｓ／Ｗ５Ｂが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またバイオメトリクス取得装置６はユーザ端末５に接続されており、上述した実施の形態１と全く同様の構成である。また認証サーバ３も、上述した実施の形態１と全く同様の構成である。

【００３７】ここでは、バイオメトリクス取得装置６に指紋取得装置７を使用する場合を例として説明する。

【００３８】次に動作について説明する。基本的には実施例１と同じであり、図２との対応部分に同一符号を付けた図４において、まずユーザがユーザ端末５で動作しているアプリケーションであるデータベース検索Ｓ／Ｗ５Ｅにより、機密度の高いローカルデータベース５Ｃの情報にアクセスした場合について説明する。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるデータベース検索Ｓ／Ｗ５Ｅは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証をする必要がある（ＳＰ５）。

【００３９】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋情報取得装置７から取得する（ＳＰ６）。この時他のＳ／Ｗ（認証情報を取得するドライバなどのソフトウエア）と協調して動作する場合もある。

【００４０】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂから指紋情報の取得を指示された、指紋取得装置の認証情報取得部７Ａは、ユーザから指紋情報を取得する（ＳＰ１）。この指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部７Ｂで暗号化を実施するが、まず暗号処理部７Ｂは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報を暗号化する。同時に暗号処理部７Ｂは、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する（ＳＰ２）。指紋取得装置７の公開鍵取得部７Ｃは、フロッピーディスクや、磁気カード、ＩＣカード、またはキー入力などユーザからの指示により認証サーバ３の公開鍵を得る。または指紋取得装置７が適切に管理されている場合には、認証サーバ３の公開鍵が指紋取得装置７で固定的に公開鍵取得部７Ｃに格納されており、ユーザが認知した上でその公開鍵を用いる場合もある。次に暗号処理部７Ｂは前記共通鍵を認証サーバ３の公開鍵で暗号化する（ＳＰ３）。そして、指紋取得部７Ａは、暗号化された指紋情報と、日時情報と、暗号化された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報としてユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂに転送する（ＳＰ４）。

【００４１】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂは、ユーザ名やメールアドレスなどのユーザＩＤを取得して認証情報に追加する（ＳＰ７）。

【００４２】認証依頼部５Ｄはこの認証情報を認証サーバ３の認証制御部３Ａへ転送する（ＳＰ７）。

【００４３】認証サーバ３の認証制御部３Ａは転送された認証情報を暗号処理部３Ｃで復号させ、ユーザ認証を実施する。この時暗号処理部３Ｃでは、認証サーバ３で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する（ＳＰ１２）。認証制御部３Ａは転送された認証情報に含まれる指紋情報とユーザIDと、認証サーバ３の認証情報データベース３Ｂに元々蓄積されている個人情報から指紋照合を実施する。認証制御部３Ａは、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部３Ｃに引き渡され、暗号処理部３Ｃでは認証結果のメッセージダイジェストをとり、認証サーバ３の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部３Ａへ引き渡す。認証制御部３Ａは前記暗号化されたメッセージダイジェストを認証結果に含めてユーザ端末５の認証依頼部５Ｄへ通知する（ＳＰ１３）。

【００４４】認証結果を受けたユーザ端末５の認証依頼部５Ｄは、暗号処理部５Ｆに認証結果を通知する。暗号処理部５Ｆは通知された暗号化されたメッセージダイジェストを認証サーバ３の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することにより、確かに正当な認証サーバ３からの通知であることを確認する（ＳＰ１０）。認証依頼部５Ｄは正当な認証サーバ３からの通知であることを確認結果を暗号処理部５Ｄから知らされたならば認証結果をデータベース検索Ｓ／Ｗ５Ｅに通知する。データベース検索Ｓ／Ｗ５Ｅは該認証結果により該ユーザに対してローカルデータベース５Ｃの機密度の高い情報へのアクセス許可・不許可を判定する。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう（ＳＰ１１）。

【００４５】このような構成によれば、ユーザ端末５が認証サーバ３へ個人認証を依頼する場合において、上述した実施例１と同一の効果を得ることができる。

【００４６】本実施例ではデータベース検索システム１に適用した例を示したが、データベース検索Ｓ／Ｗが、例えば経理情報管理Ｓ／Ｗなどの他のシステムを構成するアプリケーションであっても同様な効果が得られる。

【００４７】実施の形態３．この実施の形態３においては実施の形態１におけるバイオメトリクス取得装置６である指紋取得装置７の暗号処理部７Ｂと公開鍵取得部７Ｃがユーザ端末５にある形態である。

【００４８】図１との対応部分に同一符号を付けた図５では、ユーザ端末５は、Ｗｅｂサーバ端末４の情報を表示するブラウザ５Ａと、指紋情報を暗号化する暗号処理部５Ｆと、認証サーバ３の公開鍵を取得する公開鍵取得部５Ｇ、認証情報取得Ｓ／Ｗ５Ｂが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末５には、バイオメトリクス取得装置６が接続されている。また認証サーバ３とＷｅｂサーバ４は、上述した実施の形態１と全く同様の構成である。

【００４９】また、本実施の形態におけるバイオメトリクス取得装置６の取得するバイオメトリクス情報は、画像データや、静電データなど加工されていないイメージデータであっても、イメージデータから特徴などを抽出した特徴点データであってもよく、バイオメトリクス取得装置６はイメージデータを取得するだけのＣＰＵが実装されない簡易な機器であってもよい。ここでは、バイオメトリクス取得装置６に指紋取得装置７を使用する場合を例として説明する。指紋取得装置７は、画像処理等により、指紋情報を取得し、ユーザ端末に転送する指紋情報取得部７Ａで構成される。

【００５０】次に動作について説明する。基本的には実施例１と同じであり、図２との対応部分に同一符号を付けた図６において、まずユーザがユーザ端末５で動作しているアプリケーションであるブラウザ５により、Ｗｅｂサーバ４の機密度の高いＷｅｂサーバデータベース４Ａの情報にアクセスした場合について説明する（ＳＰ５）。前記機密度の高い情報のアクセス制御を行なっているアプリケーションであるＷｅｂサーバＳ／Ｗ４Ｃは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証をする必要がある。

【００５１】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂは、認証のために必要なバイオメトリクス情報である指紋情報を、指紋取得装置７から取得する（ＳＰ６）。この時他のＳ／Ｗ（認証情報を取得するドライバなどのソフトウエア）と協調して動作する場合もある。

【００５２】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂから指紋情報の取得を指示された、指紋取得装置７の指紋情報取得部７Ａは、ユーザから指紋情報を取得し（ＳＰ１）、ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂに転送する（ＳＰ４）。

【００５３】ユーザ端末５の認証情報取得Ｓ／Ｗ５Ｂは、指紋情報は、ユーザ固有の個人的な情報であるため、暗号処理部５Ｆで暗号化を実施させる。まず暗号処理部５Ｆは、この指紋情報を暗号化するための共通鍵方式の共通鍵を生成し、この共通鍵により指紋情報を暗号化する。同時に暗号処理部５Ｆは、日時情報を取得し、日時情報と共通鍵を連結してメッセージダイジェストを取り、そのメッセージダイジェストをさらに共通鍵で暗号化する。（ＳＰ２）。ユーザ端末５の公開鍵取得部５Ｇは、ハードディスクや、フロッピーディスク、磁気カード、ＩＣカード、またはキー入力などユーザからの指示により認証サーバの公開鍵を得る。次に暗号処理部５Ｆは前記共通鍵を認証サーバ３の公開鍵で暗号化する（ＳＰ３）。そして、認証情報取得Ｓ／Ｗ５Ｂは、暗号化された指紋情報と、日時情報と、暗号化された日時情報と共通鍵を連結してメッセージダイジェストと、暗号化された共通鍵を認証情報として、ブラウザ５Ａを介してＷｅｂサーバ４へ取得した認証情報を転送する。この時、ブラウザ５Ａは別途取得したユーザ名やメールアドレスなどのユーザＩＤを認証情報に追加して転送する（ＳＰ７）。

【００５４】Ｗｅｂサーバ４の認証依頼部４ＢはＷｅｂサーバＳ／Ｗ４Ｃを介して、取得した認証情報を認証サーバ３の認証制御部３Ａへ転送する（ＳＰ９）。

【００５５】認証サーバ３の認証制御部３Ａは転送された認証情報を暗号処理部３Ｃで復号させ、ユーザ認証を実施する。この時暗号処理部３Ｃでは、認証サーバ３で転送された日時情報と共通鍵からメッセージダイジェストを作成したものと、暗号化された日時情報と共通鍵を連結したメッセージダイジェストを復号したものを比較して、転送遅延を考慮した上で認証情報作成日時の正当性を確認する（ＳＰ１２）。認証制御部３Ａは転送された認証情報に含まれる指紋情報とユーザIDと、認証サーバ３の認証情報データベース３Ｂに元々蓄積されている個人情報から指紋照合を実施する。認証制御部３Ａは、照合した結果本人と同定した場合には、正規ユーザを示す認証結果を生成し、照合の結果本人と同定できなければ、本人ではないと判断し認証結果を生成する。この認証結果は、暗号処理部３Ｃに引き渡され、暗号処理部３Ｃでは認証結果のメッセージダイジェストをとり、認証サーバ３の秘密鍵で暗号化、すなわちデジタル署名を行い、この暗号化されたメッセージダイジェストを認証制御部３Ａへ引き渡す。認証制御部３Ａは前記暗号化されたメッセージダイジェストを認証結果に含めてＷｅｂサーバ４の認証依頼部４Ｂへ通知する（ＳＰ１３）。

【００５６】認証結果を受けたＷｅｂサーバ４の認証依頼部４Ｂは、暗号処理部４Ｄに認証結果を通知する。暗号処理部４Ｄは通知された暗号化されたメッセージダイジェストを認証サーバ３の公開鍵で復号し、通知された認証結果のメッセージダイジェストと比較することにより、確かに正当な認証サーバ３からの通知であることを確認する（ＳＰ１０）。認証依頼部４Ｂは正当な認証サーバ３からの通知であることを確認したことを暗号処理部４Ｄから知らされたならば認証結果をＷｅｂサーバＳ／Ｗ４Ｃに通知する。ＷｅｂサーバＳ／Ｗ４Ｃは該認証

結果により該ユーザに対してＷｅｂサーバデータベース４Ａの機密度の高い情報へのアクセス許可・不許可を判定する。たとえば、該機密情報の表示を行なうなど、ユーザアクセスに対する動作を行なう（ＳＰ１１）。

【００５７】このように、ユーザの個人情報である指紋情報は生成した共通鍵で暗号化され、該共通鍵は、ユーザが設定した認証サーバ３の公開鍵により暗号化されることと、認証サーバ３の公開鍵はユーザ端末５にユーザが直接設定するため、指紋情報はユーザの指定した認証サーバ３にのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報である指紋情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果がある。ただし、指紋情報がユーザ端末５では暗号化されずに存在する期間が生じるため、指紋取得装置７から暗号化される場合に比べてはセキュリティが低くなるが、ユーザ端末５自身が適切に管理されている場合には問題なく、指紋取得装置７に暗号処理部と公開鍵取得部が不要なため指紋取得装置７の構成が簡単になるという効果がある。前記した効果以外は、上述した実施例１と同様の効果を得ることができる。また、実施の形態２で示した、データベース検索Ｓ／Ｗ５Ｅなどのアプリケーションへも同様に適用でき、上述した同様の効果を得ることができる。

【００５８】また、実施の形態１や、実施の形態２、実施の形態３の全ての場合において、取得したユーザのバイオメトリクス情報を暗号化するための共通鍵を生成を行うが、この共通鍵の解読を困難にするためには、共通鍵を生成するための乱数に傾向なくす必要がある。バイオメトリクス情報は一般に取得毎に異なった値をもつことから、取得したバイオメトリクス情報のメッセージダイジェストを乱数の一部または全部として利用する。

【００５９】以上のように、取得したバイオメトリクス情報のメッセージダイジェストから生成する乱数を生成するので、生成した乱数の傾向をなくすことが簡単にできる。そして、この乱数の一部または全部を共通鍵の生成するための乱数として使用するので、認証回数や時刻などには全く関連ない乱数を発生させることができ、共通鍵の解読に対してセキュリティ上強固なシステムを構築することが可能である。

【００６０】実施の形態４．前記してきた、バイオメトリクス情報取得装置の管理は正当な管理者のみが実施できるが、正当な管理者を誰も認証できない状態に陥った場合には、前記認証されない管理者または管理を代行する他の者がバイオメトリクス取得装置の初期化を実行できる必要がある。この場合を実施の形態１と実施の形態２の指紋取得装置で、指紋取得装置が適切に管理されており、認証サーバの公開鍵が指紋取得装置で固定的に決まっている場合を例にして説明する。

【００６１】図７は、指紋取得装置１２の公開鍵取得部１２Ｃに固定的に格納される公開鍵を設定および変更など管理時の構成である。管理端末１１は管理Ｓ／Ｗ１１Ａが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。指紋取得装置１２は指紋情報取得部１２Ａと暗号処理部１２Ｂ、公開鍵取得部１２Ｃと、管理部１２Ｄで構成される。

【００６２】管理端末１１の管理Ｓ／Ｗ１１Ａは公開鍵設定を実行するため、指紋取得装置１２に管理者の認証要求を発行する。指紋取得装置１２の管理部１２Ｄの管理者認証部１２Ｄ１では、指紋情報取得部７Ａから管理者の指紋を取得し管理者の指紋照合を行うが管理者と同定できない事態が発生したような状態に陥ることがありえる。これは管理者の怪我により、指紋自体がなくなってしまった場合などが相当する。この場合、管理Ｓ／Ｗ１１Ａは指紋取得装置１２の管理部１２Ｄの初期化者認証部１２Ｄ２に対して初期化を命じるが、この時初期化用のパスワードなど事前に設定された手段により初期化者の認証を行う。初期化者認証部１２Ｄ２は初期化者のみの認証しかせず、初期化者認証部１２Ｄ２で認証時は指紋取得装置の初期化のみが実行できる。このように初期化者のための認証手段を通常の管理者と別に備えることにより、管理者が認証できなくなった場合や、管理者が突然いなくなったなどの場合においても初期化だけは実行できるとともに、初期化権限を保持していない者に不正に初期化されてしまうことを防げるという効果がある。

【００６３】実施の形態５．図８は、前述した認証サーバに、信頼性を向上するために不正認証を発見する手段を適用したものである。認証サーバ１３は、履歴部１３Ｄと、認証制御部１３Ａ、暗号処理部１３Ｃと、認証情報データベース１３Ｂから構成されるパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【００６４】認証サーバ１３の履歴部１３Ｄはユーザ認証時に、バイオメトリクスを照合した結果の照合率の履歴をとる。また、履歴部１３Ｄは、同一ユーザ認証時で認証制御部１３Ａが本人と同定しない場合には、前回までのユーザを本人と同定した時の平均照合率と比較し、今回の照合率が管理者の定める規定値以上に大きく変動しないことを確認する。履歴部１３Ｄは、既定値以上に変動している場合には失敗回数を増加させる。そして失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている管理者やユーザ自身に通知する。

【００６５】この機構によれば、管理者に対してや、成り済まされようとしているユーザに対して、バイオメトリクス認証特有の異常な照合結果を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。

【００６６】また、バイオメトリクスによる認証では、照合率が同一であってもバイオメトリクス情報は取得の

たびに異なった情報になるため、過去に取得したバイオメトリクス情報が一致することは確率的に非常に小さい。このバイオメトリクス認証の特徴を利用した不正発見の機構を説明する。図８の認証サーバ１３の履歴部１３Ｄはユーザ認証時、認証制御部１３Ａが本人と同定した場合には、前回までのユーザを本人と同定した時の照合率と比較し、同一の照合率であるかを確認する。同一であり、バイオメトリクス情報のメッセージダイジェストが格納されていない場合にはユーザ認証を失敗とすることを認証制御部１３Ａに通知し、認証制御部１３Ａは認証結果を失敗とする。同時に履歴部１３Ｄはバイオメトリクス情報のメッセージダイジェストを照合率とともに格納する。同一の照合率で、メッセージダイジェストが格納されている場合には、今回のバイオメトリクス情報のメッセージダイジェストを算出し、過去の同一の照合率におけるバイオメトリクス情報のメッセージダイジェストと比較し、異なれば本人と同定するが、一致していれば成り済まされている可能性があるためユーザ認証を失敗とすることを認証制御部１３Ａに通知する。認証制御部１３Ａは認証失敗の認証結果を失敗とする。履歴部１３Ｄは、照合率とメッセージダイジェストが一致して認証が失敗させた場合には照合率同一での失敗回数を増加させ、この失敗回数が管理者の定める既定値以上に達した場合には、予め登録されている管理者やユーザ自身に通知する。

【００６７】この機構によれば、管理者に対してや、成り済まされようとしているユーザに対して、バイオメトリクス情報の漏洩による成り済ましと考えられる異常事態を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。また、履歴部１３Ｄが記憶するのは２回目以降の同率照合率時のバイオメトリクス情報のメッセージダイジェストであるため、格納のための領域を削減できるという効果と、メッセージダイジェストによる比較のため、バイオメトリクス情報そのものを比較する場合にくらべて、比較に費やすの時間を短くできるという効果がある。

【００６８】

【発明の効果】以上のように、この発明によれば、ユーザの個人情報であるバイオメトリクス情報は暗号化され、バイオメトリクス情報はユーザの指定した認証サーバにのみ復号可能な状態でネットワーク上を転送されることになるので、バイオメトリクス情報というユーザ個人のプライバシーを、ユーザの意志を反映した形で確実に保護できるという効果があるとともに、認証サーバ３で認証情報作成時の日時が確認できるため、不正な認証情報の再使用が防止でき、さらに認証サーバによって認証されたかが認証依頼側で確認できるためシステムのセキュリティを高く保つことが可能である。

【００６９】さらに、ユーザは認証サーバの公開鍵を指示するが、仮にこの公開鍵を格納しているフロッピーディスクや、磁気カード、ＩＣカードなどが紛失や盗難にあってもセキュリティ上問題がなく、同じ公開鍵を格納した代替え品や同一品により個人認証を受けることができるとともに、公開鍵を格納している代替え品はユーザ毎に管理されているものではないため、紛失や盗難時に特別な届け出や再発行などの処理が不要であり、管理負荷が軽減できるという効果もある。

【００７０】また、取得したバイオメトリクス情報から共通鍵の生成するための乱数を生成するので、認証回数や時刻などには全く関連ない乱数を発生させることができ、共通鍵の解読に対してセキュリティ上強固なシステムを構築することが可能である。また、初期化者のための認証手段を通常の管理者と別に備えることにより、管理者が突然いなくなった場合などの場合においても初期化ができるとともに、初期化権限を保持していない者に不正に初期化されてしまうことを防げるという効果がある。

【００７１】また、認証サーバはユーザ認証時の履歴をとり、予め指定された者に対して、バイオメトリクス認証特有の異常な照合結果を通知するので、不正な認証の早期発見を可能にし、システムのセキュリティを高く保持することができる。

【図面の簡単な説明】

【図１】　この発明による遠隔認証システムを適用したＷｅｂシステムの実施の形態１の構成を示すブロック図である。

【図２】　図１のＷｅｂシステムにおける認証の処理の説明に供するタイミングチャートである。

【図３】　この発明による遠隔認証システムを適用したデータベース検索システムの実施の形態２の構成を示すブロック図である。

【図４】　図３のデータベース検索システムにおける認証の処理の説明に供するタイミングチャートである。

【図５】　この発明による遠隔認証システムを適用したＷｅｂシステムの実施の形態３の構成を示すブロック図である。

【図６】　図５のＷｅｂシステムにおける認証の処理の説明に供するタイミングチャートである。

【図７】　この発明による遠隔認証システムを適用した指紋取得装置の管理時の実施の形態４の構成を示すブロック図である。

【図８】　この発明による遠隔認証システムを適用した認証サーバの実施の形態５の構成を示すブロック図である。

【符号の説明】

１　Ｗｅｂシステム
２　ネットワーク
３　認証サーバ
３Ａ　認証制御部
３Ｂ　認証情報データベース

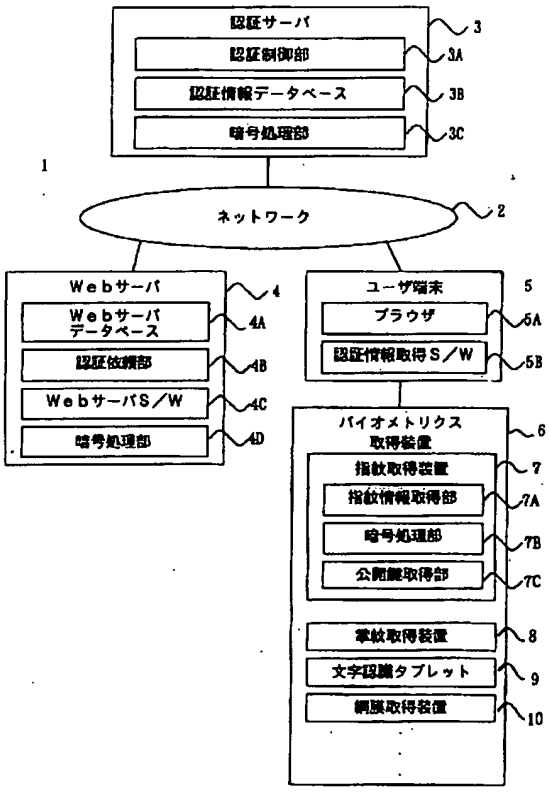
19

３Ｃ　暗号処理部
４　Ｗｅｂサーバ
４Ａ　Ｗｅｂサーバデータベース
４Ｂ　認証依頼部
４Ｃ　Ｗｅｂサーバソフトウェア
４Ｄ　暗号処理部
５　ユーザ端末
５Ａ　ブラウザ
５Ｂ　認証情報取得ソフトウェア
５Ｃ　ローカルデータベース
５Ｄ　認証依頼部
５Ｅ　データベース検索ソフトウェア
５Ｆ　暗号処理部
５Ｇ　公開鍵取得部
６　バイオメトリクス取得装置
７　指紋取得装置
７Ａ　指紋情報取得部
７Ｂ　暗号処理部

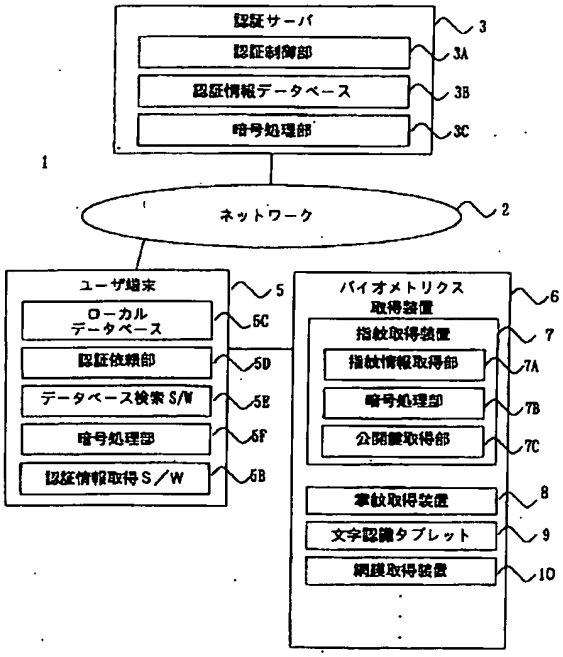
20

７Ｃ　公開鍵取得部
８　掌紋取得装置
９　文字認識タブレット
１０　網膜取得装置
１１　ユーザ端末
１１Ａ　管理ソフトウェア
１２　指紋取得装置
１２Ａ　指紋情報取得部
１２Ｂ　暗号処理部
１２Ｃ　公開鍵取得部
１２Ｄ　管理部
１２Ｄ１　管理者認証部
１２Ｄ２　初期化者認証部
１３　認証サーバ
１３Ａ　認証制御部
１３Ｂ　認証情報データベース
１３Ｃ　暗号処理部
１３Ｄ　履歴部

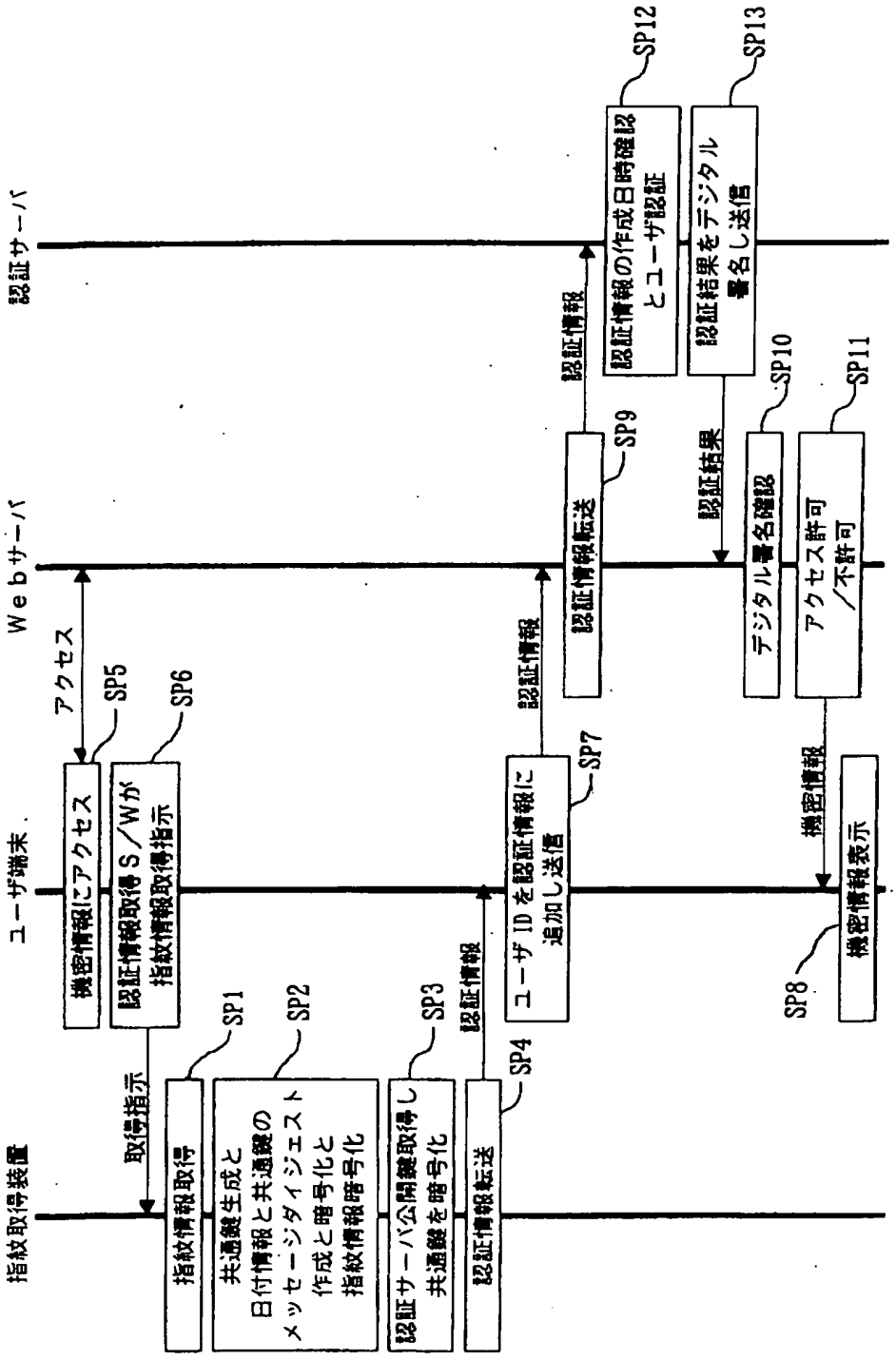
【図１】



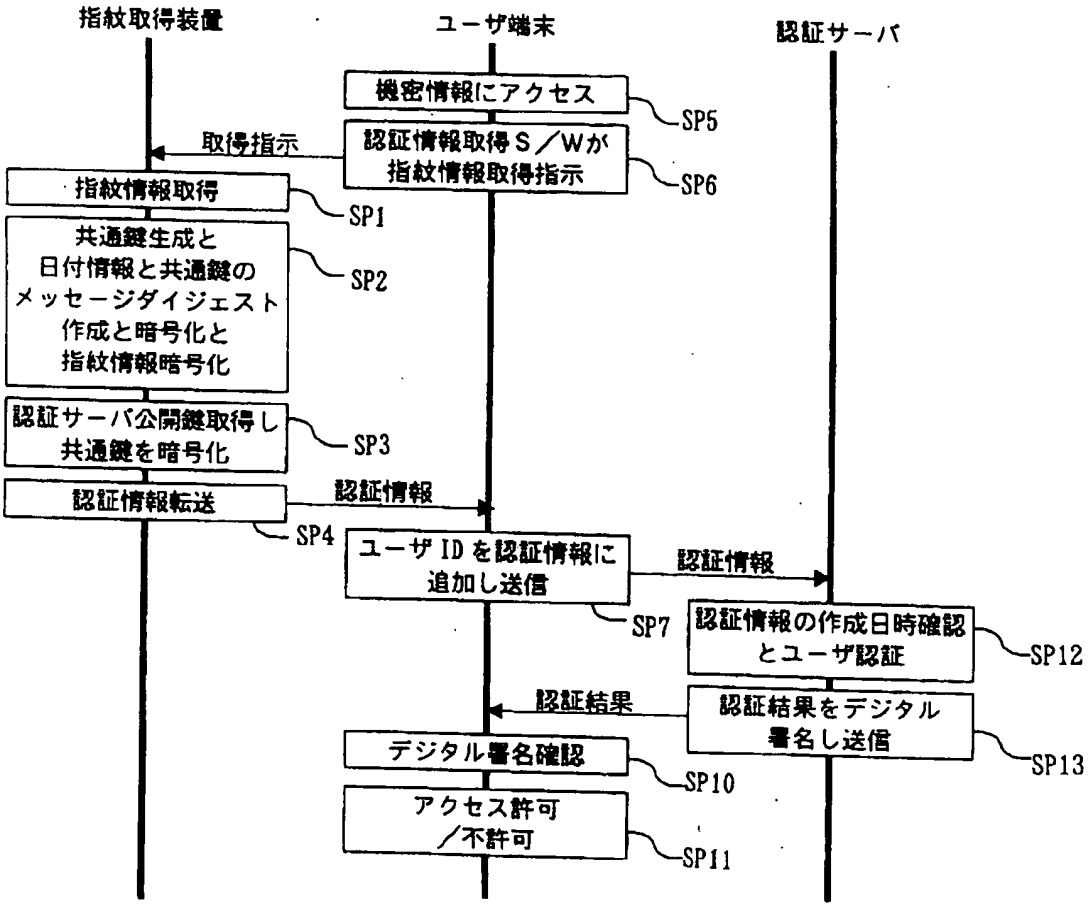

【図３】



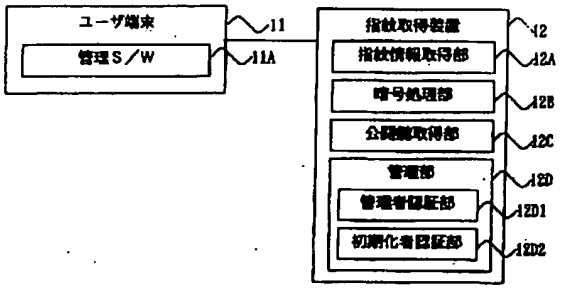
【図２】


指紋取得装置
ユーザ端末
Ｗｅｂサーバ
認証サーバ
取得指示
アクセス
機密情報にアクセス
認証情報取得Ｓ／Ｗが指紋情報取得指示
指紋情報取得
共通鍵生成と日付情報と共通鍵のメッセージダイジェスト作成と暗号化と指紋情報暗号化
認証サーバ公開鍵取得し共通鍵を暗号化
認証情報転送
認証情報
ユーザＩＤを認証情報に追加し送信
認証情報転送
認証情報の作成日時確認とユーザ認証
認証結果をデジタル署名し送信
認証結果
デジタル署名確認
アクセス許可／不許可
機密情報
機密情報表示
SP1
SP2
SP3
SP4
SP5
SP6
SP7
SP8
SP9
SP10
SP11
SP12
SP13

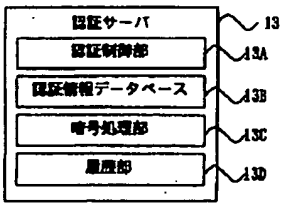
【図４】


指紋取得装置
ユーザ端末
認証サーバ
機密情報にアクセス
SP5
取得指示
認証情報取得Ｓ／Ｗが
指紋情報取得指示
SP6
指紋情報取得
SP1
共通鍵生成と
日付情報と共通鍵の
メッセージダイジェスト
作成と暗号化と
指紋情報暗号化
SP2
認証サーバ公開鍵取得し
共通鍵を暗号化
SP3
認証情報転送
認証情報
SP4
ユーザＩＤを認証情報に
追加し送信
認証情報
SP7
認証情報の作成日時確認
とユーザ認証
SP12
認証結果
認証結果をデジタル
署名し送信
SP13
デジタル署名確認
SP10
アクセス許可
／不許可
SP11

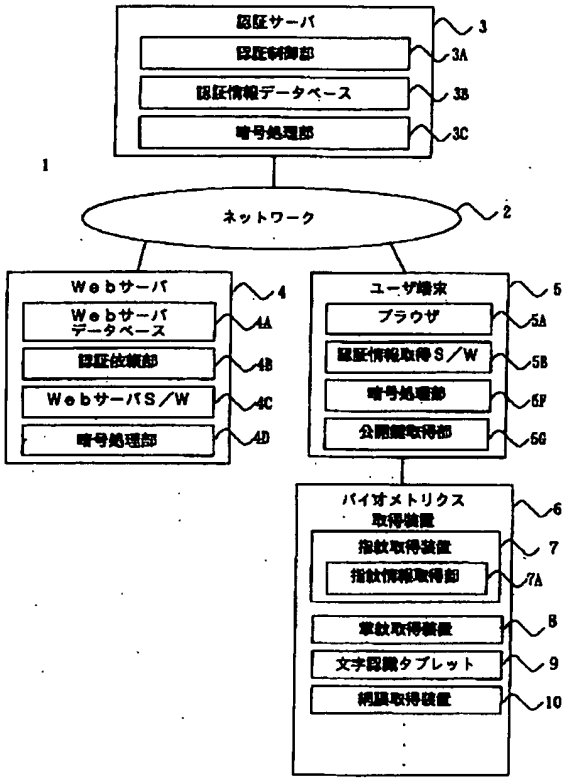
【図７】


ユーザ端末
11
管理Ｓ／Ｗ
11A
指紋取得装置
12
指紋情報取得部
12A
暗号処理部
12B
公開鍵取得部
12C
管理部
12D
管理者認証部
12D1
初期化者認証部
12D2

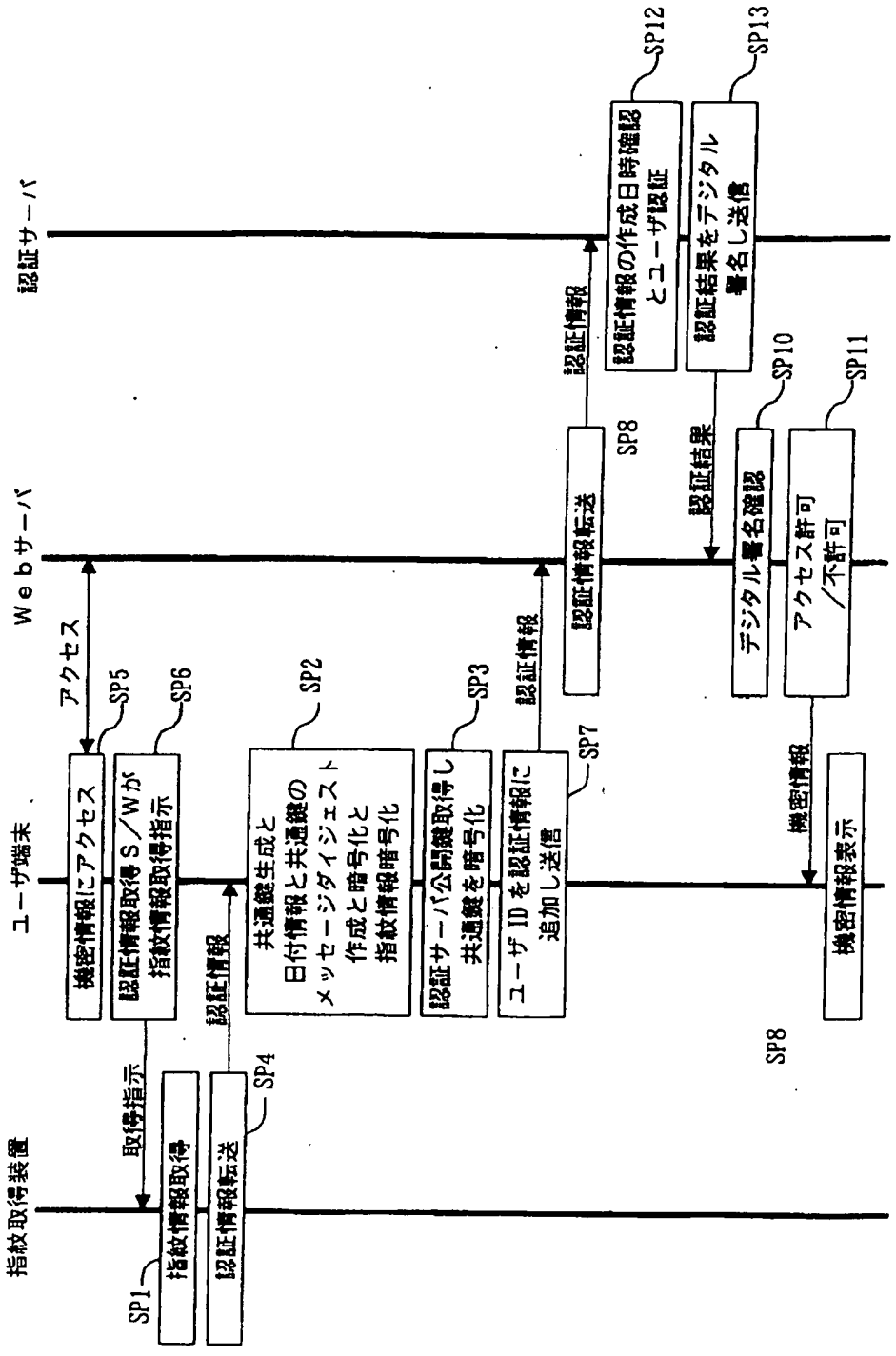
【図８】


認証サーバ
13
認証制御部
13A
認証情報データベース
13B
暗号処理部
13C
履歴部
13D

【図５】


認証サーバ
3
認証制御部
3A
認証情報データベース
3B
暗号処理部
3C
1
ネットワーク
2
Webサーバ
4
Webサーバ
データベース
4A
認証依頼部
4B
WebサーバS／W
4C
暗号処理部
4D
ユーザ端末
5
ブラウザ
5A
認証情報取得S／W
5B
暗号処理部
5F
公開鍵取得部
5G
バイオメトリクス
取得装置
6
指紋取得装置
7
指紋情報取得部
7A
掌紋取得装置
8
文字認識タブレット
9
網膜取得装置
10

【図６】


認証サーバ
Ｗｅｂサーバ
ユーザ端末
指紋取得装置
アクセス
機密情報にアクセス
SP5
認証情報取得Ｓ／Ｗが
指紋情報取得指示
SP6
取得指示
指紋情報取得
SP1
認証情報
認証情報転送
SP4
共通鍵生成と
日付情報と共通鍵の
メッセージダイジェスト
作成と暗号化と
指紋情報暗号化
SP2
認証サーバ公開鍵取得し
共通鍵を暗号化
SP3
認証情報
ユーザＩＤを認証情報に
追加し送信
SP7
認証情報転送
SP8
認証情報
認証情報の作成日時確認
とユーザ認証
SP12
認証結果をデジタル
署名し送信
SP13
認証結果
デジタル署名確認
SP10
アクセス許可
／不許可
SP11
機密情報
機密情報表示
SP8

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | F I | | テーマコード(参考) |
|---|---|---|---|---|
| | | Ｈ０４Ｌ　9/00 | ６７５Ｄ | |

(72)発明者　貞包　哲男
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　藤井　照子
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Ｆターム(参考)　5B043 AA09 BA02 BA03 BA04 BA06 CA09 FA02 HA20
5B085 AC03 AE06 AE13 AE23 AE25 AE29 BG07
5J104 AA07 EA01 EA19 KA01 KA16 MA02 NA02 PA07